UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/765,719	01/26/2004	Yolanta Beresnevichiene	200207541-2	2569

22879 7590 04/29/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/29/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/765,719	BERESNEVICHIENE ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-12,17-20,22-29,31-33,36 and 38-41* is/are rejected.

7)☒ Claim(s) *13-16,21,30,34,35 and 37* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on 01/29/2009, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Claim Objections

2. Claims 3, & 22 are objected to because of the following informalities:

- Claim 22 line 9 recites "a" which should be omitted;

3. Claim 3 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 3 has been amended to depend from Claim 6, however, 3 cannot come after 6 and it appears that Claim 3 was meant to have been renumbered.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1 line 8 recites "a predetermined system call" however, it is unclear as to whether this is a separate "predetermined system call" or the same as the earlier recited one;

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 4, 5, 7, 22, 25-27, 39, 40, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meyers et al. (US-5937159).

Claim 1:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, but they do not explicitly disclose,

- "a system call monitor for detecting predetermined system calls and data manipulated by the process so as to modify identifiable characteristics of the data," although Meyers et al. do suggest an authentication daemon changing authentication data, as recited below;
- "means for applying a data handling policy upon detecting: a predetermined data type based on a tag or label associated with the data manipulated by the process or based on the format of the data manipulated by the process," although Meyers et al. do suggest access control policies between subjects (i.e. process) and system objects (i.e. data) utilizing mandatory access control labels or tuples, as recited below;
- "a predetermined system call which involves the writing of data outside the process," although Meyers et al. do suggest printing data out, as recited below;

however, Meyers et al. do disclose,

- "The authentication daemon can perform a number of functions upon request: (a) It can check to see if a user is authentic. The particular authentication data used and the means used to authenticate the user depend on the particular AD. (b) It can change the authentication data…" [column 4 lines 36-49];
- "Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object… MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…" [column 6 lines 9-32];
- "…It can print the data or convert it to some other human readable form, for example, ASCII text…" [column 4 lines 45-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a system call monitor for detecting predetermined system calls and data manipulated by the process so as to modify identifiable characteristics of the data" and

"means for applying a data handling policy upon detecting: a predetermined data type based on a tag or label associated with the data manipulated by the process or based on the format of the data manipulated by the process" and "a predetermined system call which involves the writing of data outside the process," in the invention as disclosed by Meyers et al. for the purposes of providing process access control to data without having to implement large monolithic processes.

Claim 4:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 1 above, further comprising,

- "predetermined system calls are those involving the transmission of data externally of the computing platform" (i.e. "…It can print the data or convert it to some other human readable form, for example, ASCII text…") [column 4 lines 45-46].

Claim 5:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 1 above, further comprising,

- "means for applying a data handling policy comprises a tag determiner for determining any security tags associated with the data manipulated by the process or based on the format of the data manipulated by the process handled by the system call" and "means for applying a data handling policy comprises a policy interpreter for determining a policy according to any such tags and for applying the policy" (i.e. "…Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the

subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object…MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…") [column 6 lines 9-32].

Claim 7:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 1 above, further comprising,

- "the policy interpreter comprises a policy database including tag policies" and "the policy interpreter comprises a policy reconciler for generating a composite policy from the tag policies relevant to the data" (i.e. "…Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object…MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of

users) following the syntax: hierarchy: (category1, category2 . . .)...") [column 6 lines 9-32].

Claim 22:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, but they do not explicitly disclose,

- "detecting both a predetermined data type based on a tag or label associated with the data or based on the format of the data," although Meyers et al. do suggest an authentication daemon changing authentication data, as recited below;
- "predetermined system calls involving the writing of data outside the process," although Meyers et al. do suggest printing data out, as recited below;
- "applying a data handling policy to a system call upon both said predetermined data type and said predetermined system call being detected," although Meyers et al. do suggest access control policies between subjects (i.e. process) and system objects (i.e. data) utilizing mandatory access control labels or tuples, as recited below;
- "the data handling policy being applied for all system calls involving the writing of data outside the process," although Meyers et al. do suggest printing data out, as recited below;

however, Meyers et al. do disclose,

- "The authentication daemon can perform a number of functions upon request: (a) It can check to see if a user is authentic. The particular authentication data used and the means

used to authenticate the user depend on the particular AD. (b) It can change the authentication data…" [column 4 lines 36-49];

- "Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object… MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…" [column 6 lines 9-32];
- "…It can print the data or convert it to some other human readable form, for example, ASCII text…" [column 4 lines 45-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "detecting both a predetermined data type based on a tag or label associated with the data or based on the format of the data" and "predetermined system calls involving the writing of data outside the process" and "applying a data handling policy to a system call upon both said predetermined data type and said predetermined system call being detected" and "the data handling policy being applied for all system calls involving the writing

of data outside the process," in the invention as disclosed by Meyers et al. for the purposes of providing process access control to data without having to implement large monolithic processes.

Claim 25:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 22 above, further comprising,

- "predetermined system calls are those involving the transmission of data externally of the computing platform" (i.e. "…It can print the data or convert it to some other human readable form, for example, ASCII text…") [column 4 lines 45-46].

Claim 26:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 22 above, further comprising,

- "determining any security tags associated with data handled by the system call" and "determining a policy according to any such tags and applying the policy" (i.e. "…Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object…MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The

label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…") [column 6 lines 9-32].

Claim 27:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 22 above, further comprising,

- "a composite policy is generated from the tag policies relevant to the data" (i.e. "…Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object…MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…") [column 6 lines 9-32].

Claims 39 & 40:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 22 above, further comprising,

- "a computer program stored in computer readable media for controlling a computing platform to operate in accordance with claim 22" and "a computer platform configured to operate according to claim 22" [FIG 3 illustrates software stored on hardware which performs steps similar to claim 22].

Claim 41:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, but they do not explicitly disclose,

- "a system call monitor for detecting predetermined system calls and data handled by the process," although Meyers et al. do suggest an authentication daemon changing authentication data, as recited below;
- "a policy applicator for applying a data handling policy to the system call upon both a predetermined data type based on a tag or label associated with the data handled by the process or based on the format of the data handled by the process," although Meyers et al. do suggest access control policies between subjects (i.e. process) and system objects (i.e. data) utilizing mandatory access control labels or tuples, as recited below;
- "a predetermined system call which involves the writing of data outside the process," although Meyers et al. do suggest printing data out, as recited below;

however, Meyers et al. do disclose,

- "The authentication daemon can perform a number of functions upon request: (a) It can check to see if a user is authentic. The particular authentication data used and the means

used to authenticate the user depend on the particular AD. (b) It can change the authentication data…" [column 4 lines 36-49];

- "Access Control Policies… mandatory access control is an access policy that controls a subject's access to information and objects. The system enforces the policy by comparing the sensitivity of the information for the object (its MAC label or MAC tuple) to the MAC tuple of the subject's process…compares the object's sensitivity to the MAC label of the subject's process…relationship of the MAC label and the MAC tuple determines if a subject can read an object, write to an object, or is denied access to the object… MAC label--a label placed on subjects and objects in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)…" [column 6 lines 9-32];
- "…It can print the data or convert it to some other human readable form, for example, ASCII text…" [column 4 lines 45-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a system call monitor for detecting predetermined system calls and data handled by the process" and "a policy applicator for applying a data handling policy to the system call upon both a predetermined data type based on a tag or label associated with the data handled by the process or based on the format of the data handled by the process" and "applying a data handling policy to a system call upon both said predetermined data type and said predetermined system call being detected" and "a predetermined system call which involves the writing of data outside the process," in the invention as disclosed by Meyers et al. for the

purposes of providing process access control to data without having to implement large monolithic processes.

8. Claims 3, 6, 23, 24, & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meyers et al. (US-5937159) in view of Choo (US-6981140-B1).

Claim 6:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 5 above, but do not disclose,

- "the policy interpreter is configured to use the intended destination of the data as a factor in determining the policy for the data," although Choo does suggest policy enforcement/access control based on where data packets come from, as recited below;

however, Choo does disclose,

- "For incoming data packets received from the remote host across a LAN/WAN each packet received from the operating system is inspected to see if internet protocol security decryption is necessary by examining a security descriptor data comprising a part of a security association data logically associated with the data packet" [column 12 lines 54-59];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the policy interpreter is configured to use the intended

destination of the data as a factor in determining the policy for the data," in the invention as disclosed by Meyers et al. for the purposes of enforcing policies/access control.

Claim 23:

Meyers et al. disclose a data handling apparatus and method for a computer platform using an operating system executing a process, as in Claim 22 above respectively, but do not disclose,

- "the policy is to require the encryption of at least some of the data," although Choo does suggest encryption of data, as recited below;

however, Choo does disclose,

- "the security database associated with key database 602 is consulted to determine whether the data packet received from user process 600 is to be encrypted prior to transmission across the network" [column 13 lines 14-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the policy is to require the encryption of at least some of the data," in the invention as disclosed by Meyers et al. for the purposes of securing the data.

Claims 3 & 24:

Meyers et al. disclose a data handling apparatus and method for a computer platform using an operating system executing a process, as in Claims 1 and 23 above respectively, but do not disclose,

- "the policy interpreter in its application of the policy automatically encrypts the at least some of the data," although Choo does suggest encryption of data, as recited below;

however, Choo does disclose,

- "the security database associated with key database 602 is consulted to determine whether the data packet received from user process 600 is to be encrypted prior to transmission across the network" [column 13 lines 14-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a policy interpreter in its application of the policy automatically encrypts the at least some of the data," in the invention as disclosed by Meyers et al. for the purposes of securing the data.

Claim 28:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 26 above, but do not disclose,

- "the intended destination of the data is used as a factor in determining the policy for the data," although Choo does suggest policy enforcement/access control based on where data packets come from, as recited below;

however, Choo does disclose,

- "For incoming data packets received from the remote host across a LAN/WAN each packet received from the operating system is inspected to see if internet protocol security decryption is necessary by examining a security descriptor data comprising a part of a security association data logically associated with the data packet" [column 12 lines 54-59];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the intended destination of the data is used as a factor in determining the policy for the data," in the invention as disclosed by Meyers et al. for the purposes of enforcing policies/access control.

9. Claims 8-12, 17-20, 29, 31-33, & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meyers et al. (US-5937159) in view of Yoshioka et al. (US-5909688-A).

Claims 8 & 29:

Meyers et al. disclose a data handling apparatus and method for a computer platform using an operating system executing a process, as in Claims 1 and 22 above respectively, but do not disclose,

- "the computing platform comprises a data management unit," although Yoshioka et al. do suggest a data management unit, as recited below;
- "the data management unit arranged to associate data management information with data input to a process," although Yoshioka et al. do suggest entity information corresponding with each record, as recited below;
- "(the data management unit arranged to) regulate operating system operations involving the data according to the data management information," although Yoshioka et al. do suggest controlling read/write of data, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit];

- "in a record of department in an entity management table corresponding to the above-mentioned organization template there are stored entity information corresponding to that record, an XID value of, for example, a technical department, a pointer to a section record which is a low-rank record, a pointer to a record for another department which is in the same rank as that department, and a pointer to that department which is the entity information item" [column 6 lines 9-17];
- " The data management unit 24 controls reading or writing of data between the database 25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the computing platform comprises a data management unit" and "the data management unit arranged to associate data management information with data input to a process" and "(the data management unit arranged to) regulate operating system operations involving the data according to the data management information," in the invention as disclosed by Meyers et al. for the purposes of associating and tracking data processed in an operating system.

Claim 9:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the computing platform further comprises a memory space," although Yoshioka et al. do suggest a memory, as recited below;

- "the computing platform is arranged to load the process into the memory space," although Yoshioka et al. do suggest a memory connected to other components for data processes, as recited below;
- "the computing platform is arranged to run the process under the control of the data management unit," although Yoshioka et al. do suggest a data management unit, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a memory arranged with other components to load and handle data processes and a data management unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the computing platform further comprises a memory space" and "the computing platform is arranged to load the process into the memory space" and "the computing platform is arranged to run the process under the control of the data management unit," in the invention as disclosed by Meyers et al. for the purposes of loading a process into memory and handling the execution of that process according to a policy, as are common elements of an operating system's functionality when incorporated according to a system as shown in Fig 13 of Yoshioka et al.

Claim 10:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the data management information is associated with at least one data sub-unit as data is input to a process from a data unit comprising a plurality of sub-units," although Yoshioka et al. do suggest a data management unit connected to additional components, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a system with a data management unit and several sub-units defining aspects of policy, work-flow, etc interfaced with an interface unit, a database, and a memory];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management information is associated with at least one data sub-unit as data is input to a process from a data unit comprising a plurality of sub-units," in the invention as disclosed by Meyers et al. since the data management unit would associate data according to the policies of the subunits as data input for the purposes of handling data processing.

Claim 11:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "data management information is associated with each independently addressable data unit," although Yoshioka et al. do suggest a data management unit controlling the read/write of data involving memory, as recited below;

however, Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database 25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "data management information is associated with each independently addressable data unit," in the invention as disclosed by Meyers et al. since the data management unit would have some association or elements of data identification for the purposes of reading/writing data between a database and memory.

Claim 12:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the data management unit comprises part of an operating system kernel space," although Yoshioka et al. do suggest a data management unit, as recited below;

however, Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database 25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management unit comprises part of an operating system kernel space," in the invention as disclosed by Meyers et al. since reading/writing to memory and between a database is typically an operation reserved for kernel space privileges, for the purposes of resource access control within the operating system.

Claim 17:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the data management unit comprises a data filter to identify data management information associated with data that is to be read into the memory space," although Yoshioka et al. do suggest a data management unit reading/writing data between a database and memory, as recited below;

however, Yoshioka et al. do disclose,

- "The data management unit 24 controls reading or writing of data between the database 25 and the memory 31" [column 12 lines 65-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management unit comprises a data filter to identify data management information associated with data that is to be read into the memory space," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory, for the purposes of ensuring data integrity/consistency between what is in memory and what is written in the database.

Claim 18:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the data management unit further comprises a tag management module arranged to allow a user to specify data management information to be associated with data," although Yoshioka et al. do suggest a data management unit connected to an interface unit, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates an interface unit interfaced with the data management unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management unit further comprises a tag management module arranged to allow a user to specify data management information to be associated with data," in the invention as disclosed by Meyers et al. for the purpose of allowing additional policies/control over the data management unit.

Claim 19:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 8 above, but do not disclose,

- "the data management unit comprises a tag propagation module arranged to maintain an association with the data that has been read into the process and the data management information associated therewith," although Yoshioka et al. do suggest a data management unit connected with several additional components for data management, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data management unit comprises a tag propagation module arranged to maintain an association with the data that has been read into the process and the data management information associated therewith," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency between data in memory and the data written in the database.

Claim 20:

Meyers et al. disclose a data handling apparatus for a computer platform using an operating system executing a process, as in Claim 19 above, but do not disclose,

- "the tag propagation module is arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations," although Yoshioka et al. do suggest a data management unit in association with a policy unit, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the tag propagation module is arranged to maintain an

association between an output of operations carried out within the process and the data management information associated with the data involved in the operations," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency between data in memory and the data written in the database, as well as, access control for the data.

Claim 31:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but do not disclose,

- "associating data management information with data as the data is read into a memory space," although Yoshioka et al. do suggest a data management unit in association with a policy unit and a memory, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "associating data management information with data as the data is read into a memory spaces," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order

to read/write data between the database and memory for the purposes of data integrity/consistency in memory.

Claim 32:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but do not disclose,

- "associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units," although Yoshioka et al. do suggest a data management unit in association with a policy unit and a memory, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory for the purposes of data integrity/consistency between data in memory and the data written in the database, as well as, access control for the data.

Claim 33:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but do not disclose,

- "associating data management information with each independently addressable data unit that is read into the memory space," although Yoshioka et al. do suggest a data management unit in association with a memory, as recited below;

however, Yoshioka et al. do disclose,

- [Fig 13 illustrates a data management unit interfaced with a database, memory, and several subunits including a policy unit];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "associating data management information with each independently addressable data unit that is read into the memory space," in the invention as disclosed by Meyers et al. since the data management unit would have to have some association or elements of data identification in order to read/write data between the database and memory.

Claim 36:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but do not disclose,

- "the step (b) comprises sub-steps," although Yoshioka et al. do suggest a database in association with additional sub-components including a policy unit, as recited below;
- "identifying an operation involving the data," although Yoshioka et al. do suggest a database in association with additional sub-components including a policy unit, as recited below;

- "if the operation involves the data and is carried out within the process, maintaining an association between an output of the operation and the data management information," although Yoshioka et al. do suggest a database in association with additional sub-components including a policy unit, as recited below;
- "if the operation involving the data includes a write operation to a location external to the process, selectively performing the operation dependent on the data management information," although Yoshioka et al. do suggest a database in association with additional sub-components including a policy unit, as recited below;

however, Yoshioka et al. does disclose,

- [Fig 14 illustrates several subunits that perform sub-steps and interact with a database];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the step (b) comprises sub-steps" and "identifying an operation involving the data" and "if the operation involves the data and is carried out within the process, maintaining an association between an output of the operation and the data management information" and "if the operation involving the data includes a write operation to a location external to the process, selectively performing the operation dependent on the data management information," in the invention as disclosed by Meyers et al. since database read/write sessions typically involve multiple steps (i.e. sub-steps) and involve data operations. In addition, the data management unit would have some association or elements of data identification in order to read/write data between the database and memory for the purposes of maintaining data

integrity/consistency between data in memory and data written in the database, as well as, for the access control of data processing operations by the policy unit.

10. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Meyers et al. (US-5937159) in view of Johnson et al. (US-5684948-A).

Claim 38:

Meyers et al. disclose a data handling method for a computer platform using an operating system executing a process, as in Claim 29 above, but do not disclose,

- "the process instructions are analyzed as blocks," although Johnson et al. do suggest addressable privilege levels of code in each address block, as recited below;
- "each block defined by operations up to a terminating condition," although Johnson et al. do suggest bit sets indicating privilege levels, as recited below;

however, Yoshioka et al. does disclose,

- "the privilege level of the code (and/or data) in each of a plurality of address blocks addressable by the processor" [column 2 lines 41-42];
- "The bit being set indicates that the corresponding address block has one privilege level and the bit being cleared indicates that the corresponding address block has the other privilege level" [column 2 lines 46-48];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the process instructions are analyzed as blocks" and "each block defined by operations up to a terminating condition," in the invention as disclosed by Meyers et al. since process instructions are typically handled as blocks by a processor and would have a condition for completion.

Allowable Subject Matter

11. Claims 13-16, 21, 30, 34, 35 & 37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Gladstone et al. (US-20030023774-A1) – reads on a different interpretation of the independent and dependent claims based on the current claim language;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
04/24/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436